Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of generating a password for use by an end-user device (UE) to access a remote server, comprising:

sending a first request for access from the UE to the remote server;

creating a temporary identity for the UE by said remote server;

sending directly from said remote server to an authentication node in the UE's home network a second request for access, said second request including said temporary identity for the UE and an identity of said remote server;

determining if said remote server is authorized to send a second request for access;

at the authentication node, generating a challenge to said UE said challenge including details of the temporary identity of the UE and said identity of said remote server;

at the authentication node, generating a first password based on said temporary identity of the UE and said identity of said remote server;

at the UE, generating a second password based on the identity of the remote server and the temporary identity of the UE included in said received challenge;

storing the second password and the temporary identity of the UE at the UE;

sending an authentication response from said UE including a proof of possession of the second password thereby establishing authentication between said UE and said remote server; and

in response to said authentication response from said UE, the authentication node sending a request response back to the remote server, said response including the first password, allowing said remote server and said UE to challenge and authenticate a subsequent access request directly without sending said second request from said remote server to said authentication node.

2. (Previously Presented) The method in claim 1, wherein said authentication node uses HTTP Digest Authentication and Key Agreement (AKA) for generating said first password.

3-5. (Cancelled)

6. (Previously Presented) The method in claim 1, wherein a HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE.

7. (Cancelled)

8. (Previously Presented) The method in claim 1, further comprising authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the first password has been generated.

9-12. (Cancelled)

13. (Previously Presented) The method in claim 1, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server.

14. (Previously Presented) The method in claim 1, further comprising authenticating the UE at the authentication node and returning an authentication result to the remote server.

15-17. (Cancelled)

18. (Currently Amended) A method of authentication an end-user device (UE) with a remote server, comprising the steps of:

receiving a first request for access from said UE by said remote server;

creating a temporary identity for the UE by said remote server;

sending directly from said remote server to an authentication node in the UE's home network a second request for access, said second request including said temporary identity created by said remote server and an identity of said remote server and instructing said authentication node to generate a challenge to said UE, said challenge including said temporary identity of the UE and said identity of said remote server;

determining if said remote server is authorized to send a second request for access;

at the UE, generating a password based on the challenge, said password being associated with the temporary identity of the UE created by said remote server;

storing the password and the temporary identity of the UE at the UE;

receiving at said remote server a first authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server and allowing said remote server and said UE to challenge and authenticate a subsequent access request directly without sending said second request from said remote server to said authentication node.

19-22. (Cancelled)

23. (Previously Presented) The method in claim 18, wherein the challenge generated by the authentication node is an HTTP Digest challenge.

24. (Previously Presented) The method in claim 23, wherein the password is stored at the authentication node.

25. (Previously Presented) The method in claim 23, further comprising authenticating the UE at the authentication node and redirecting the request for access

from the authentication node to the remote server after the password has been generated.

26-29. (Cancelled)

30. (Previously Presented) The method in claim 23, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server.

31-33. (Cancelled)

* * *